



Memorandum

To: Rules Committee

From: Councilmember Pete Constant

Subject: SAN JOSE PUBLIC
LIBRARY INTERNET
ACCESS AND COMPUTER
USE POLICY

Date: October 18, 2007

Approved:

RECOMMENDATION

1. I recommend that the Rules Committee direct staff to agendize a discussion and direction to the City Manager, regarding Internet use at San José Public Libraries for November 6, 2007.
2. I recommend that the Rules Committee forward the following policy to the City Council as a proposal for ensuring safe and child-sensitive Internet use at San José Public Libraries.

BACKGROUND

The City of San José has an award-winning library system that serves the needs of San José residents as well those of our neighboring communities. San José public libraries provide integral early and elementary educational resources through children's story time, Artscard Program, Events for Kids, KidsPlace Gateway, Reading to Children, Summer Reading Celebration and homework centers. The City of San José partnered with residents by passing a multi-million dollar sales tax measure that provided unprecedented investment in San José's library system in 2000.

Parents expect San José public libraries to be child-safe community resources for learning and discovery. However, the libraries do not protect children from viewing pornographic and obscene images on the Internet or from others who are publicly viewing such material. It is unlikely that this is the kind of "education" parents expect their children to get at San José Libraries.

We have spent countless hours working to protect our children from second-hand smoke in parks, but have done nothing to protect them from the dangers of "second-hand porn" and, in some cases, the lewd acts performed by individuals viewing obscene material in public. Instead, the City seeks to protect porn-viewers' rights to view obscene material. If library staff receives a complaint from other library users about someone viewing obscene material, current policy

leaves it within the discretion of library staff whether to require the porn-viewer simply to screen their monitor, which merely lessens the likelihood of second-hand porn viewing, but does not eliminate it. In some cases complainants may be asked to avert their eyes to protect the porn-viewer's rights.

The following excerpts from the San José Library Department's current Internet use policy (Attachment A) reflect the aforementioned failure to protect minors who may have come to their local library for any one of the multitude of programs geared toward children.

[T]he Library does not monitor and has no control over the information accessed through the Internet and assumes no responsibility for its content.

The Library neither restricts access to materials found on the Internet nor protects users from materials or information they may find offensive. The Library encourages all users to make appropriate use of the Internet by providing programs and assistance for responsible use.

Parents or legal guardians must assume responsibility for deciding what library resources are appropriate for their own children. It is both the right and the responsibility of parents and legal guardians to guide their own children's usage of library resources in accordance with individual family beliefs.

Privacy screens are available in all branches and units of the Library, and may be requested by customers for use in the library. *In addition, a staff member may require a customer to use a privacy screen when a staff member deems it necessary.*

The City's negligence in protecting children from inadvertently viewing obscene material is in violation of the 2000 Children's Internet Protection Act (Attachment B). The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes requirements on any school or library that receives funding support for Internet access or internal connections from the "E-rate" program – a program that makes certain technology more affordable for eligible schools and libraries. In early 2001, the Federal Communications Commission (FCC) issued rules implementing CIPA. These rules require:

- Schools and libraries subject to CIPA may not receive the discounts offered by the E-Rate program unless they certify that they have an Internet safety policy and technology protection measures in place. *An Internet safety policy must include technology protection measures to block or filter Internet access to pictures that: (a) are obscene, (b) are child pornography, or (c) are harmful to minors, for computers that are accessed by minors.*
- Schools and libraries subject to CIPA are required to adopt and implement a policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and

dissemination of personal information regarding minors; and (e) *restricting minors' access to materials harmful to them.*

Schools and libraries are required to certify that they have their safety policies and technology in place before receiving E-rate funding. However:

- CIPA does not affect E-rate funding for schools and libraries receiving discounts only for telecommunications, such as telephone service.
- An authorized person may disable the blocking or filtering measure during any use by an adult to enable access for *bona fide* research or other lawful purposes.

Many jurisdictions have taken appropriate measures to protect children from second-hand porn by installing filtering software. Phoenix, Houston, Baltimore County, Minneapolis, Denver, Sacramento, San Diego, Santa Cruz, Fresno and Shasta County have all instituted policies that filter Internet use to better protect children. These jurisdictions' policies are summarized in Attachment C.

There is court precedent supporting these policies. In 2003, the United States Supreme Court heard a challenge to the constitutionality of the CIPA and upheld local municipalities' rights to use Internet filters in Public Libraries, ruling that this kind of filtering is not a violation of the First Amendment. In *U.S. v. American Library Association, Inc.*, the court affirmed the precedent that "...the Government has broad discretion to make content-based judgments in deciding what private speech to make available to the public." Furthermore, the Court found that "[t]he decisions by most libraries to exclude pornography from their print collections are not subjected to heightened scrutiny; it would make little sense to treat libraries' judgments to block online pornography any differently." Attachment D is a summary of the court's decision.

ANALYSIS

Almost a year ago, an ABC 7 I-Team report exposed San José's failure to protect children from pornography and those who would openly view pornographic material in their presence (Attachments E & F). The investigation revealed that there have been a number of individuals arrested for viewing child pornography in libraries, and still others have been arrested for performing lewd acts such as masturbating in public while viewing pornographic material. According to recent police reports these were not isolated incidents, yet nothing has been done to make libraries safe for kids to be kids. It is time that we take action. San José's children should be free to discover the world in libraries without having to sacrifice their innocence.

The proposed Internet use policy as outlined in attachment G has been drafted to fit within the CIPA and Supreme Court's framework for filtering inappropriate material, while allowing adults access to filtered content on an as-needed basis for legitimate research. It will protect children from the effects of second-hand porn and the exposure to the lewd acts that some individuals have engaged in while viewing obscene material in public.

The proposed policy has been drafted in coordination with the Alliance Defense Fund (ADF). If adopted as proposed, the ADF has agreed to defend the City of San José to legal challenges, free of charge, up to, and including, the U.S. Supreme Court.

The City has developed a tool called [My Rules for Internet Safety](#) to help parents protect their children from Internet predators and inadvertently viewing obscene material. However, the City has not yet taken the appropriate action to protect children at public libraries. If San José is to be a *Family-Friendly City* then the next logical step is to assist parents by ensuring that children are protected from the negative affects of second-hand porn.

CONCLUSION

Parents expect libraries to be child-safe environments. It is within our authority, and our ability, to take reasonable measures to ensure that children are no longer subjected to obscene material and lewd acts in San José Public Libraries; therefore we have a moral imperative to do so.

Federal law, and common sense, require filtering programs and child-friendly Internet-use policies be instituted in order to qualify for federal funding. As we seek to close a multi-million dollar structural budget deficit, it is our fiscal responsibility to ensure that the City of San José is competitive when seeking outside funding to ensure that we are providing our residents with access to the latest software and hardware. The City is not currently taking full advantage of the funding available.

Other jurisdictions have been successful in instituting similar policies and while it is disappointing that San José has not taken the lead in protecting children from second-hand porn, there is nothing stopping us from joining other morally conscious municipalities. We owe it to the community to be a family friendly city.

Attachment A

Current City Internet Access Policy

The Dr. Martin Luther King Jr. Library and the San José Public Library system provide access to the Internet in accordance with their mission of providing public access to information of all types in a wide range of formats. In doing so, the Library does not monitor and has no control over the information accessed through the Internet and assumes no responsibility for its content.

The Internet is a global electronic network. It enables the Library to greatly expand its information services beyond the traditional collections and resources. However, not all information on the Internet is current, complete or accurate. The Internet may contain material of a controversial or mature nature. The Library neither restricts access to materials found on the Internet nor protects users from materials or information they may find offensive. The Library encourages all users to make appropriate use of the Internet by providing programs and assistance for responsible use.

Parents or legal guardians must assume responsibility for deciding what library resources are appropriate for their own children. It is both the right and the responsibility of parents and legal guardians to guide their own children's usage of library resources in accordance with individual family beliefs. The library has created Web pages for children ([KidsPlace](#)) and young adults ([TeenWeb](#)) which provide content and links to other Web sites that parents and legal guardians may find appropriate for their children. For more information on children and the Internet, see [My Rules for Internet Safety](#).

My Rules for Internet Safety

I will follow my parents' rules for going online:

- *I will tell my parents or teachers about any email messages, Web sites, or other online experiences that upset me in any way.*
- *People I meet online are strangers. Unless I have my parents' permission: I will not give out information, such as my name, my parents' name, my address, my telephone number, my school name or other information about myself or my family.*
- *I will not get together in person with anyone I've met online.*
- *I will not send anyone I've met online a picture of myself or of my family.*

SJLibrary.org offers access to information resources over the Internet in order to be responsive to the information needs of our diverse community. While the Library strives to offer sites which provide current and accurate information, the changing nature of this medium means the Library cannot guarantee the accuracy of information gained through the World Wide Web. Users are responsible for determining that the information they access is acceptable, reliable and suitable to their needs.

It is a violation of federal law to knowingly receive visual depictions of minors engaged in sexually explicit conduct. Anyone who does so is subject to federal criminal prosecution under the Protection of Children Against Sexual Exploitation Act of 1977(18 USC 2252).

Materials obtained or copied on Library computers may be subject to copyright laws which govern the making of reproductions of copyrighted works. Users must comply with U.S. copyright law and other applicable laws.

Rules Governing In-House Use

1. Due to the limited resources available for provision of public access to the Internet, the Library reserves the right to limit the amount of time an individual user may have access to library equipment.
2. Rules for use of the Library's Internet workstations are posted near or on terminals, and include reservation information, time limits on usage of machines, and limits on printing.
3. Library staff members will assist customers, as time permits, with basic Internet navigation and with basic computer and printer functions.
4. Users may not attempt to reconfigure systems or software, or in any way interfere with or disrupt the current system or network set-up and services.
5. Users may not unplug, remove, or otherwise modify library equipment.
6. Some workstations have a dedicated purpose, such as searching for periodical citations and articles, and are to be used only for that dedicated purpose. Some workstations are reserved for use by children or for use by people with disabilities.
7. Privacy screens are available in all branches and units of the Library, and may be requested by customers for use in the library. In addition, a staff member may require a customer to use a privacy screen when a staff member deems it necessary.
8. Users may not invade the privacy of others. Each customer has the right to a quiet and organized work space. No more than two people may use a work station at the same time.
9. If any user abuses or engages in unauthorized use of computers, his or her computer privileges will be denied. If a customer refuses a staff request to end problem behavior, the customer will be asked to leave the library. Staff may call upon the assistance of other and/or supervisory staff, and if the situation escalates, Public Safety staff or police may be called.
10. Computers will be shut down no later than 5 minutes before the Library closes.

Attachment B

TITLE XVII--CHILDREN'S INTERNET PROTECTION

SEC. 1701. SHORT TITLE.

This title may be cited as the ``Children's Internet Protection Act''.

SEC. 1702. DISCLAIMERS.

(a) **DISCLAIMER REGARDING CONTENT.**--Nothing in this title or the amendments made by this title shall be construed to prohibit a local educational agency, elementary or secondary school, or library from blocking access on the Internet on computers owned or operated by that agency, school, or library to any content other than content covered by this title or the amendments made by this title.

(b) **DISCLAIMER REGARDING PRIVACY.**--Nothing in this title or the amendments made by this title shall be construed to require the tracking of Internet use by any identifiable minor or adult user.

SEC. 1703. STUDY OF TECHNOLOGY PROTECTION MEASURES.

(a) **IN GENERAL.**--Not later than 18 months after the date of the enactment of this Act, the National Telecommunications and Information Administration shall initiate a notice and comment proceeding for purposes of--

- (1) evaluating whether or not currently available technology protection measures, including commercial Internet blocking and filtering software, adequately addresses the needs of educational institutions;
- (2) making recommendations on how to foster the development of measures that meet such needs; and
- (3) evaluating the development and effectiveness of local Internet safety policies that are currently in operation after community input.

(b) **DEFINITIONS.**--In this section:

(1) **TECHNOLOGY PROTECTION MEASURE.**--The term ``technology protection measure'' means a specific technology that blocks or filters Internet access to visual depictions that are--

- (A) obscene, as that term is defined in section 1460 of title 18, United States Code;
- (B) child pornography, as that term is defined in section 2256 of title 18, United States Code; or
- (C) harmful to minors.

(2) **HARMFUL TO MINORS.**--The term ``harmful to minors'' means any picture, image, graphic image file, or other visual depiction that--

- (A) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- (B) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
- (C) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

(3) **SEXUAL ACT; SEXUAL CONTACT.**--The terms ``sexual act'' and ``sexual contact'' have the meanings given such terms in section 2246 of title 18, United States Code.

Subtitle A--Federal Funding for Educational Institution Computers

SEC. 1711. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS.

Title III of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 6801 et seq.) is amended by adding at the end the following:

``PART F--LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS

``SEC. 3601. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS.

``(a) INTERNET SAFETY.--

``(1) IN GENERAL.--No funds made available under this title to a local educational agency for an elementary or secondary school that does not receive services at discount rates under section 254(h)(5) of the Communications Act of 1934, as added by section 1721 of Children's Internet Protection Act, may be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet, for such school unless the school, school board, local educational agency, or other authority with responsibility for administration of such school both--

``(A)(i) has in place a policy of Internet safety for minors that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--

``(I) obscene;

``(II) child pornography; or

``(III) harmful to minors; and

``(ii) is enforcing the operation of such technology protection measure during any use of such computers by minors; and

``(B)(i) has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--

``(I) obscene; or

``(II) child pornography; and

``(ii) is enforcing the operation of such technology protection measure during any use of such computers.

``(2) TIMING AND APPLICABILITY OF IMPLEMENTATION.--

``(A) IN GENERAL.--The local educational agency with responsibility for a school covered by paragraph (1) shall certify the compliance of such school with the requirements of paragraph (1) as part of the application process for the next program funding year under this Act following the effective date of this section, and for each subsequent program funding year thereafter.

``(B) PROCESS.--

``(i) SCHOOLS WITH INTERNET SAFETY POLICIES AND TECHNOLOGY PROTECTION MEASURES IN PLACE.--A local educational agency with responsibility for a school covered by paragraph (1) that has in place an Internet safety policy meeting the requirements of paragraph (1) shall certify its compliance with paragraph (1) during each annual program application cycle under this Act.

``(ii) SCHOOLS WITHOUT INTERNET SAFETY POLICIES AND TECHNOLOGY PROTECTION MEASURES IN PLACE.--A local educational agency with responsibility for a school covered by paragraph (1) that does not have in place an Internet safety policy meeting the requirements of paragraph (1)--

“(I) for the first program year after the effective date of this section in which the local educational agency is applying for funds for such school under this Act, shall certify that it is undertaking such actions, including any necessary procurement procedures, to put in place an Internet safety policy that meets such requirements; and

“(II) for the second program year after the effective date of this section in which the local educational agency is applying for funds for such school under this Act, shall certify that such school is in compliance with such requirements.

Any school covered by paragraph (1) for which the local educational agency concerned is unable to certify compliance with such requirements in such second program year shall be ineligible for all funding under this title for such second program year and all subsequent program years until such time as such school comes into compliance with such requirements.

“(iii) **WAIVERS.**--Any school subject to a certification under clause (ii)(II) for which the local educational agency concerned cannot make the certification otherwise required by that clause may seek a waiver of that clause if State or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required by that clause. The local educational agency concerned shall notify the Secretary of the applicability of that clause to the school. Such notice shall certify that the school will be brought into compliance with the requirements in paragraph (1) before the start of the third program year after the effective date of this section in which the school is applying for funds under this title.

“(3) **DISABLING DURING CERTAIN USE.**--An administrator, supervisor, or person authorized by the responsible authority under paragraph (1) may disable the technology protection measure concerned to enable access for bona fide research or other lawful purposes.

“(4) **NONCOMPLIANCE.**--

“(A) **USE OF GENERAL EDUCATION PROVISIONS ACT REMEDIES.**--

Whenever the Secretary has reason to believe that any recipient of funds under this title is failing to comply substantially with the requirements of this subsection, the Secretary may--

“(i) withhold further payments to the recipient under this title,

“(ii) issue a complaint to compel compliance of the recipient through a cease and desist order, or

“(iii) enter into a compliance agreement with a recipient to bring it into compliance with such requirements,

in same manner as the Secretary is authorized to take such actions under sections 455, 456, and 457, respectively, of the General Education Provisions Act (20 U.S.C. 1234d).

“(B) **RECOVERY OF FUNDS PROHIBITED.**--The actions authorized by subparagraph (A) are the exclusive remedies available with respect to the failure of a school to comply substantially with a provision of this subsection, and the Secretary shall not seek a recovery of funds from the recipient for such failure.

“(C) **RECOMMENCEMENT OF PAYMENTS.**--Whenever the Secretary determines (whether by certification or other appropriate evidence) that a recipient of funds who is subject to the withholding of payments under subparagraph (A)(i) has cured the failure providing the basis for the withholding of payments, the Secretary shall cease the withholding of payments to the recipient under that subparagraph.

“(5) **DEFINITIONS.**--In this section:

``(A) **COMPUTER.**--The term `computer' includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer.

``(B) **ACCESS TO INTERNET.**--A computer shall be considered to have access to the Internet if such computer is equipped with a modem or is connected to a computer network which has access to the Internet.

``(C) **ACQUISITION OR OPERATION.**--A elementary or secondary school shall be considered to have received funds under this title for the acquisition or operation of any computer if such funds are used in any manner, directly or indirectly--

``(i) to purchase, lease, or otherwise acquire or obtain the use of such computer; or

``(ii) to obtain services, supplies, software, or other actions or materials to support, or in connection with, the operation of such computer.

``(D) **MINOR.**--The term `minor' means an individual who has not attained the age of 17.

``(E) **CHILD PORNOGRAPHY.**--The term `child pornography' has the meaning given such term in section 2256 of title 18, United States Code.

``(F) **HARMFUL TO MINORS.**--The term `harmful to minors' means any picture, image, graphic image file, or other visual depiction that--

``(i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

``(ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

``(iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

``(G) **OBSCENE.**--The term `obscene' has the meaning given such term in section 1460 of title 18, United States Code.

``(H) **SEXUAL ACT; SEXUAL CONTACT.**--The terms `sexual act' and `sexual contact' have the meanings given such terms in section 2246 of title 18, United States Code.

``(b) **EFFECTIVE DATE.**--This section shall take effect 120 days after the date of the enactment of the Children's Internet Protection Act.

``(c) **SEPARABILITY.**--If any provision of this section is held invalid, the remainder of this section shall not be affected thereby."

SEC. 1712. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR LIBRARIES.

(a) **AMENDMENT.**--Section 224 of the Museum and Library Services Act (20 U.S.C. 9134(b)) is amended--

(1) in subsection (b)--

(A) by redesignating paragraph (6) as paragraph (7); and

(B) by inserting after paragraph (5) the following new paragraph:

``(6) provide assurances that the State will comply with subsection (f); and"; and

(2) by adding at the end the following new subsection:

``(f) **INTERNET SAFETY.**--

``(1) **IN GENERAL.**--No funds made available under this Act for a library described in section 213(2)(A) or (B) that does not receive services at discount rates under section 254(h)(6) of the Communications Act of 1934, as added by section 1721 of this

Children's Internet Protection Act, may be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet, for such library unless--

``(A) such library--

``(i) has in place a policy of Internet safety for minors that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--

``(I) obscene;

``(II) child pornography; or

``(III) harmful to minors; and

``(ii) is enforcing the operation of such technology protection measure during any use of such computers by minors; and

``(B) such library--

``(i) has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--

``(I) obscene; or

``(II) child pornography; and

``(ii) is enforcing the operation of such technology protection measure during any use of such computers.

``(2) **ACCESS TO OTHER MATERIALS.**--Nothing in this subsection shall be construed to prohibit a library from limiting Internet access to or otherwise protecting against materials other than those referred to in subclauses (I), (II), and (III) of paragraph (1)(A)(i).

``(3) **DISABLING DURING CERTAIN USE.**--An administrator, supervisor, or other authority may disable a technology protection measure under paragraph (1) to enable access for bona fide research or other lawful purposes.

``(4) **TIMING AND APPLICABILITY OF IMPLEMENTATION.**--

``(A) **IN GENERAL.**--A library covered by paragraph (1) shall certify the compliance of such library with the requirements of paragraph (1) as part of the application process for the next program funding year under this Act following the effective date of this subsection, and for each subsequent program funding year thereafter.

``(B) **PROCESS.**--

``(i) **LIBRARIES WITH INTERNET SAFETY POLICIES AND**

TECHNOLOGY PROTECTION MEASURES IN PLACE.--A library covered by paragraph (1) that has in place an Internet safety policy meeting the requirements of paragraph (1) shall certify its compliance with paragraph (1) during each annual program application cycle under this Act.

``(ii) **LIBRARIES WITHOUT INTERNET SAFETY POLICIES AND**

TECHNOLOGY PROTECTION MEASURES IN PLACE.--A library covered by paragraph (1) that does not have in place an Internet safety policy meeting the requirements of paragraph (1)--

``(I) for the first program year after the effective date of this subsection in which the library applies for funds under this Act, shall certify that it is undertaking such actions, including any necessary procurement procedures, to put in place an Internet safety policy that meets such requirements; and

``(II) for the second program year after the effective date of this subsection in which

the library applies for funds under this Act, shall certify that such library is in compliance with such requirements.

Any library covered by paragraph (1) that is unable to certify compliance with such requirements in such second program year shall be ineligible for all funding under this Act for such second program year and all subsequent program years until such time as such library comes into compliance with such requirements.

``(iii) **WAIVERS.**--Any library subject to a certification under clause (ii)(II) that cannot make the certification otherwise required by that clause may seek a waiver of that clause if State or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required by that clause. The library shall notify the Director of the Institute of Museum and Library Services of the applicability of that clause to the library. Such notice shall certify that the library will comply with the requirements in paragraph (1) before the start of the third program year after the effective date of this subsection for which the library is applying for funds under this Act.

``(5) **NONCOMPLIANCE.**--

``(A) **USE OF GENERAL EDUCATION PROVISIONS ACT REMEDIES.**--

Whenever the Director of the Institute of Museum and Library Services has reason to believe that any recipient of funds this Act is failing to comply substantially with the requirements of this subsection, the Director may--

``(i) withhold further payments to the recipient under this Act,

``(ii) issue a complaint to compel compliance of the recipient through a cease and desist order, or

``(iii) enter into a compliance agreement with a recipient to bring it into compliance with such requirements.

``(B) **RECOVERY OF FUNDS PROHIBITED.**--The actions authorized by subparagraph (A) are the exclusive remedies available with respect to the failure of a library to comply substantially with a provision of this subsection, and the Director shall not seek a recovery of funds from the recipient for such failure.

``(C) **RECOMMENCEMENT OF PAYMENTS.**--Whenever the Director determines (whether by certification or other appropriate evidence) that a recipient of funds who is subject to the withholding of payments under subparagraph (A)(i) has cured the failure providing the basis for the withholding of payments, the Director shall cease the withholding of payments to the recipient under that subparagraph.

``(6) **SEPARABILITY.**--If any provision of this subsection is held invalid, the remainder of this subsection shall not be affected thereby.

``(7) **DEFINITIONS.**--In this section:

``(A) **CHILD PORNOGRAPHY.**--The term 'child pornography' has the meaning given such term in section 2256 of title 18, United States Code.

``(B) **HARMFUL TO MINORS.**--The term 'harmful to minors' means any picture, image, graphic image file, or other visual depiction that--

``(i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

``(ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

``(iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to

minors.

``(C) **MINOR**.--The term `minor' means an individual who has not attained the age of 17.

``(D) **OBSCENE**.--The term `obscene' has the meaning given such term in section 1460 of title 18, United States Code.

``(E) **SEXUAL ACT; SEXUAL CONTACT**.--The terms `sexual act' and `sexual contact' have the meanings given such terms in section 2246 of title 18, United States Code."

(b) **EFFECTIVE DATE**.--The amendment made by this section shall take effect 120 days after the date of the enactment of this Act.

Subtitle B--Universal Service Discounts

SEC. 1721. REQUIREMENT FOR SCHOOLS AND LIBRARIES TO ENFORCE INTERNET SAFETY POLICIES WITH TECHNOLOGY PROTECTION MEASURES FOR COMPUTERS WITH INTERNET ACCESS AS CONDITION OF UNIVERSAL SERVICE DISCOUNTS.

(a) **SCHOOLS**.--Section 254(h) of the Communications Act of 1934 (47 U.S.C. 254(h)) is amended--

(1) by redesignating paragraph (5) as paragraph (7); and

(2) by inserting after paragraph (4) the following new paragraph (5):

``(5) **REQUIREMENTS FOR CERTAIN SCHOOLS WITH COMPUTERS HAVING INTERNET ACCESS**.--

``(A) **INTERNET SAFETY**.--

``(i) **IN GENERAL**.--Except as provided in clause (ii), an elementary or secondary school having computers with Internet access may not receive services at discount rates under paragraph (1)(B) unless the school, school board, local educational agency, or other authority with responsibility for administration of the school--

``(I) submits to the Commission the certifications described in subparagraphs (B) and (C);

``(II) submits to the Commission a certification that an Internet safety policy has been adopted and implemented for the school under subsection (I); and

``(III) ensures the use of such computers in accordance with the certifications.

``(ii) **APPLICABILITY**.--The prohibition in clause (i) shall not apply with respect to a school that receives services at discount rates under paragraph (1)(B) only for purposes other than the provision of Internet access, Internet service, or internal connections.

``(iii) **PUBLIC NOTICE; HEARING**.--An elementary or secondary school described in clause (i), or the school board, local educational agency, or other authority with responsibility for administration of the school, shall provide reasonable public notice and hold at least 1 public hearing or meeting to address the proposed Internet safety policy. In the case of an elementary or secondary school other than an elementary or secondary school as defined in section 14101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 8801), the notice and hearing required by this clause may be limited to those members of the public with a relationship to the school.

``(B) **CERTIFICATION WITH RESPECT TO MINORS**.--A certification under this subparagraph is a certification that the school, school board, local educational agency, or other authority with responsibility for administration of the school--

``(i) is enforcing a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure with

respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--

``(I) obscene;

``(II) child pornography; or

``(III) harmful to minors; and

``(ii) is enforcing the operation of such technology protection measure during any use of such computers by minors.

``(C) **CERTIFICATION WITH RESPECT TO ADULTS.**--A certification under this paragraph is a certification that the school, school board, local educational agency, or other authority with responsibility for administration of the school--

``(i) is enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--

``(I) obscene; or

``(II) child pornography; and

``(ii) is enforcing the operation of such technology protection measure during any use of such computers.

``(D) **DISABLING DURING ADULT USE.**--An administrator, supervisor, or other person authorized by the certifying authority under subparagraph (A)(i) may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose.

``(E) **TIMING OF IMPLEMENTATION.**--

``(i) **IN GENERAL.**--Subject to clause (ii) in the case of any school covered by this paragraph as of the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certification under subparagraphs (B) and (C) shall be made--

``(I) with respect to the first program funding year under this subsection following such effective date, not later than 120 days after the beginning of such program funding year; and

``(II) with respect to any subsequent program funding year, as part of the application process for such program funding year.

``(ii) **PROCESS.**--

``(I) **SCHOOLS WITH INTERNET SAFETY POLICY AND TECHNOLOGY PROTECTION MEASURES IN PLACE.**--A school covered by clause (i) that has in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C) shall certify its compliance with subparagraphs (B) and (C) during each annual program application cycle under this subsection, except that with respect to the first program funding year after the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certifications shall be made not later than 120 days after the beginning of such first program funding year.

``(II) **SCHOOLS WITHOUT INTERNET SAFETY POLICY AND TECHNOLOGY PROTECTION MEASURES IN PLACE.**--A school covered by clause (i) that does not have in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C)--

``(aa) for the first program year after the effective date of this subsection in which it is

applying for funds under this subsection, shall certify that it is undertaking such actions, including any necessary procurement procedures, to put in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C); and

“(bb) for the second program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is in compliance with subparagraphs (B) and (C).

Any school that is unable to certify compliance with such requirements in such second program year shall be ineligible for services at discount rates or funding in lieu of services at such rates under this subsection for such second year and all subsequent program years under this subsection, until such time as such school comes into compliance with this paragraph.

“(III) **WAIVERS.**--Any school subject to subclause (II) that cannot come into compliance with subparagraphs (B) and (C) in such second year program may seek a waiver of subclause (II)(bb) if State or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required by such subclause. A school, school board, local educational agency, or other authority with responsibility for administration of the school shall notify the Commission of the applicability of such subclause to the school. Such notice shall certify that the school in question will be brought into compliance before the start of the third program year after the effective date of this subsection in which the school is applying for funds under this subsection.

“(F) **NONCOMPLIANCE.**--

“(i) **FAILURE TO SUBMIT CERTIFICATION.**--Any school that knowingly fails to comply with the application guidelines regarding the annual submission of certification required by this paragraph shall not be eligible for services at discount rates or funding in lieu of services at such rates under this subsection.

“(ii) **FAILURE TO COMPLY WITH CERTIFICATION.**--Any school that knowingly fails to ensure the use of its computers in accordance with a certification under subparagraphs (B) and (C) shall reimburse any funds and discounts received under this subsection for the period covered by such certification.

“(iii) **REMEDY OF NONCOMPLIANCE.**--

“(I) **FAILURE TO SUBMIT.**--A school that has failed to submit a certification under clause (i) may remedy the failure by submitting the certification to which the failure relates. Upon submittal of such certification, the school shall be eligible for services at discount rates under this subsection.

“(II) **FAILURE TO COMPLY.**--A school that has failed to comply with a certification as described in clause (ii) may remedy the failure by ensuring the use of its computers in accordance with such certification. Upon submittal to the Commission of a certification or other appropriate evidence of such remedy, the school shall be eligible for services at discount rates under this subsection.”

(b) **LIBRARIES.**--Such section 254(h) is further amended by inserting after paragraph (5), as amended by subsection (a) of this section, the following new paragraph:

“(6) **REQUIREMENTS FOR CERTAIN LIBRARIES WITH COMPUTERS HAVING INTERNET ACCESS.**--

“(A) **INTERNET SAFETY.**--

“(i) **IN GENERAL.**--Except as provided in clause (ii), a library having one or more

computers with Internet access may not receive services at discount rates under paragraph (1)(B) unless the library--

((I) submits to the Commission the certifications described in subparagraphs (B) and (C); and

((II) submits to the Commission a certification that an Internet safety policy has been adopted and implemented for the library under subsection (I); and

((III) ensures the use of such computers in accordance with the certifications.

((ii) **APPLICABILITY.**--The prohibition in clause (i) shall not apply with respect to a library that receives services at discount rates under paragraph (1)(B) only for purposes other than the provision of Internet access, Internet service, or internal connections.

((iii) **PUBLIC NOTICE; HEARING.**--A library described in clause (i) shall provide reasonable public notice and hold at least 1 public hearing or meeting to address the proposed Internet safety policy.

((B) **CERTIFICATION WITH RESPECT TO MINORS.**--A certification under this subparagraph is a certification that the library--

((i) is enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--

((I) obscene;

((II) child pornography; or

((III) harmful to minors; and

((ii) is enforcing the operation of such technology protection measure during any use of such computers by minors.

((C) **CERTIFICATION WITH RESPECT TO ADULTS.**--A certification under this paragraph is a certification that the library--

((i) is enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are--

((I) obscene; or

((II) child pornography; and

((ii) is enforcing the operation of such technology protection measure during any use of such computers.

((D) **DISABLING DURING ADULT USE.**--An administrator, supervisor, or other person authorized by the certifying authority under subparagraph (A)(i) may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose.

((E) **TIMING OF IMPLEMENTATION.**--

((i) **IN GENERAL.**--Subject to clause (ii) in the case of any library covered by this paragraph as of the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certification under subparagraphs (B) and (C) shall be made--

((I) with respect to the first program funding year under this subsection following such effective date, not later than 120 days after the beginning of such program funding year; and

((II) with respect to any subsequent program funding year, as part of the application process for such program funding year.

((ii) **PROCESS.**--

``(I) LIBRARIES WITH INTERNET SAFETY POLICY AND TECHNOLOGY PROTECTION MEASURES IN PLACE.--A library covered by clause (i) that has in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C) shall certify its compliance with subparagraphs (B) and (C) during each annual program application cycle under this subsection, except that with respect to the first program funding year after the effective date of this paragraph under section 1721(h) of the Children's Internet Protection Act, the certifications shall be made not later than 120 days after the beginning of such first program funding year.

``(II) LIBRARIES WITHOUT INTERNET SAFETY POLICY AND TECHNOLOGY PROTECTION MEASURES IN PLACE.--A library covered by clause (i) that does not have in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C)--

``(aa) for the first program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is undertaking such actions, including any necessary procurement procedures, to put in place an Internet safety policy and technology protection measures meeting the requirements necessary for certification under subparagraphs (B) and (C); and

``(bb) for the second program year after the effective date of this subsection in which it is applying for funds under this subsection, shall certify that it is in compliance with subparagraphs (B) and (C).

Any library that is unable to certify compliance with such requirements in such second program year shall be ineligible for services at discount rates or funding in lieu of services at such rates under this subsection for such second year and all subsequent program years under this subsection, until such time as such library comes into compliance with this paragraph.

``(III) WAIVERS.--Any library subject to subclause (II) that cannot come into compliance with subparagraphs (B) and (C) in such second year may seek a waiver of subclause (II)(bb) if State or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required by such subclause. A library, library board, or other authority with responsibility for administration of the library shall notify the Commission of the applicability of such subclause to the library. Such notice shall certify that the library in question will be brought into compliance before the start of the third program year after the effective date of this subsection in which the library is applying for funds under this subsection.

``(F) NONCOMPLIANCE.--

``(i) FAILURE TO SUBMIT CERTIFICATION.--Any library that knowingly fails to comply with the application guidelines regarding the annual submission of certification required by this paragraph shall not be eligible for services at discount rates or funding in lieu of services at such rates under this subsection.

``(ii) FAILURE TO COMPLY WITH CERTIFICATION.--Any library that knowingly fails to ensure the use of its computers in accordance with a certification under subparagraphs (B) and (C) shall reimburse all funds and discounts received under this subsection for the period covered by such certification.

``(iii) REMEDY OF NONCOMPLIANCE.--

``(I) FAILURE TO SUBMIT.--A library that has failed to submit a certification

under clause (i) may remedy the failure by submitting the certification to which the failure relates. Upon submittal of such certification, the library shall be eligible for services at discount rates under this subsection.

“(II) **FAILURE TO COMPLY.**--A library that has failed to comply with a certification as described in clause (ii) may remedy the failure by ensuring the use of its computers in accordance with such certification. Upon submittal to the Commission of a certification or other appropriate evidence of such remedy, the library shall be eligible for services at discount rates under this subsection.”

(c) **DEFINITIONS.**--Paragraph (7) of such section, as redesignated by subsection (a)(1) of this section, is amended by adding at the end the following:

“(D) **MINOR.**--The term ‘minor’ means any individual who has not attained the age of 17 years.

“(E) **OBSCENE.**--The term ‘obscene’ has the meaning given such term in section 1460 of title 18, United States Code.

“(F) **CHILD PORNOGRAPHY.**--The term ‘child pornography’ has the meaning given such term in section 2256 of title 18, United States Code.

“(G) **HARMFUL TO MINORS.**--The term ‘harmful to minors’ means any picture, image, graphic image file, or other visual depiction that--

“(i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

“(ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

“(iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

“(H) **SEXUAL ACT; SEXUAL CONTACT.**--The terms ‘sexual act’ and ‘sexual contact’ have the meanings given such terms in section 2246 of title 18, United States Code.

“(I) **TECHNOLOGY PROTECTION MEASURE.**--The term ‘technology protection measure’ means a specific technology that blocks or filters Internet access to the material covered by a certification under paragraph (5) or (6) to which such certification relates.”

(d) **CONFORMING AMENDMENT.**--Paragraph (4) of such section is amended by striking “paragraph (5)(A)” and inserting “paragraph (7)(A)”.

(e) **SEPARABILITY.**--If any provision of paragraph (5) or (6) of section 254(h) of the Communications Act of 1934, as amended by this section, or the application thereof to any person or circumstance is held invalid, the remainder of such paragraph and the application of such paragraph to other persons or circumstances shall not be affected thereby.

(f) **REGULATIONS.**--

(1) **REQUIREMENT.**--The Federal Communications Commission shall prescribe regulations for purposes of administering the provisions of paragraphs (5) and (6) of section 254(h) of the Communications Act of 1934, as amended by this section.

(2) **DEADLINE.**--Notwithstanding any other provision of law, the Commission shall prescribe regulations under paragraph (1) so as to ensure that such regulations take effect 120 days after the date of the enactment of this Act.

(g) **AVAILABILITY OF CERTAIN FUNDS FOR ACQUISITION OF**

TECHNOLOGY PROTECTION MEASURES.

(1) **IN GENERAL.**--Notwithstanding any other provision of law, funds available under section 3134 or part A of title VI of the Elementary and Secondary Education Act of 1965, or under section 231 of the Library Services and Technology Act, may be used for the purchase or acquisition of technology protection measures that are necessary to meet the requirements of this title and the amendments made by this title. No other sources of funds for the purchase or acquisition of such measures are authorized by this title, or the amendments made by this title.

(2) **TECHNOLOGY PROTECTION MEASURE DEFINED.**--In this section, the term "technology protection measure" has the meaning given that term in section 1703.

(h) **EFFECTIVE DATE.**--The amendments made by this section shall take effect 120 days after the date of the enactment of this Act.

Subtitle C--Neighborhood Children's Internet Protection

SEC. 1731. SHORT TITLE.

This subtitle may be cited as the "Neighborhood Children's Internet Protection Act".

SEC. 1732. INTERNET SAFETY POLICY REQUIRED.

Section 254 of the Communications Act of 1934 (47 U.S.C. 254) is amended by adding at the end the following:

“(1) INTERNET SAFETY POLICY REQUIREMENT FOR SCHOOLS AND LIBRARIES.--

“(1) IN GENERAL.--In carrying out its responsibilities under subsection (h), each school or library to which subsection (h) applies shall--

“(A) adopt and implement an Internet safety policy that addresses--

“(i) access by minors to inappropriate matter on the Internet and World Wide Web;

“(ii) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

“(iii) unauthorized access, including so-called 'hacking', and other unlawful activities by minors online;

“(iv) unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and

“(v) measures designed to restrict minors' access to materials harmful to minors; and

“(B) provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy.

“(2) LOCAL DETERMINATION OF CONTENT.--A determination regarding what matter is inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination.

No agency or instrumentality of the United States Government may--

“(A) establish criteria for making such determination;

“(B) review the determination made by the certifying school, school board, local educational agency, library, or other authority; or

“(C) consider the criteria employed by the certifying school, school board, local educational agency, library, or other authority in the administration of subsection (h)(1)(B).

“(3) AVAILABILITY FOR REVIEW.--Each Internet safety policy adopted under this subsection shall be made available to the Commission, upon request of the Commission, by the school, school board, local educational agency, library, or other authority responsible for adopting such Internet safety policy for purposes of the review

of such Internet safety policy by the Commission.

“(4) **EFFECTIVE DATE.**--This subsection shall apply with respect to schools and libraries on or after the date that is 120 days after the date of the enactment of the Children's Internet Protection Act.”.

SEC. 1733. IMPLEMENTING REGULATIONS.

Not later than 120 days after the date of enactment of this Act, the Federal Communications Commission shall prescribe regulations for purposes of section 254(l) of the Communications Act of 1934, as added by section 1732 of this Act.

Subtitle D--Expedited Review

SEC. 1741. EXPEDITED REVIEW.

(a) **THREE-JUDGE DISTRICT COURT HEARING.**--Notwithstanding any other provision of law, any civil action challenging the constitutionality, on its face, of this title or any amendment made by this title, or any provision thereof, shall be heard by a district court of 3 judges convened pursuant to the provisions of section 2284 of title 28, United States Code.

(b) **APPELLATE REVIEW.**--Notwithstanding any other provision of law, an interlocutory or final judgment, decree, or order of the court of 3 judges in an action under subsection (a) holding this title or an amendment made by this title, or any provision thereof, unconstitutional shall be reviewable as a matter of right by direct appeal to the Supreme Court. Any such appeal shall be filed not more than 20 days after entry of such judgment, decree, or order.

Attachment C

SAMPLE LANGUAGE FROM OTHER LIBRARY POLICIES: INTERNET FILTERING

Phoenix Public Library System: Computer and Internet Use Policy

The Library uses filtering technology on all computers with Internet access. Patrons 17 years of age or older are given a choice of an Internet session with a basic filter or one that has additional filtering. The intent of the basic option is to block websites that are considered to be pornographic. The intent of the additional filtering is to block websites that are not appropriate for children. If a patron wishes to access a site that is blocked by filtering software, that patron may request Library staff to unblock the site.

Houston Public Library System: Internet Use Policy and Guidelines

In agreement with CIPA Regulations, all Library public access workstations use filtering software to access the Internet. Adults 18 or older who need unfiltered access for any lawful purpose may request it from a staff member. Unfiltered access will be granted on a per-search basis.

Baltimore (MD) County Library System: Internet Acceptable Use Statement

The library is required by the Children's Internet Protection Act (CIPA) to prohibit Internet access for children age 16 and younger to obscenity, child pornography, and material that is harmful to minors. In order to implement the law, the library uses a Technology Protection Measure or a filtering service on all public access computers.

The filtering service disables access to certain web sites. Upon request by a library customer age 17 and older, library staff may unblock a site. Library staff may request proof of age. The library reserves the right to enforce the Acceptable Use Policy if the requested material appears to violate the law.

Minneapolis Public Library System: Internet Policy

The Children's Internet Protection Act (CIPA) passed Congress in 2000 and upheld by the Supreme Court in 2003, requires libraries receiving certain types of federal funding to equal Internet-access computers with a technology protection measure that blocks or filters visual depictions that are obscene, contain child pornography or are harmful to minors. In compliance with CIPA, the Library Board authorized installation of filtering software designed to prevent access to obscenity, child pornography and materials harmful to minors. In accordance with the law, persons aged 17 years or older may request to have the filters disabled for any lawful purpose that meets the Minneapolis Public Library Internet Policy and Guidelines and the filter will be disabled.

Denver Public Library System: Computer/Internet Policy

The Denver Public Library complies with state and federal law mandating the use of filtering software in public libraries. It employs software to protect against the depiction of illegal content. The Denver Public Library is committed to free and equal access to information. In compliance with state and federal law adults 17 or older may disable the filter on computers in the adult areas of the Library. The filtering software may not be disabled for children or on computers in designated children's areas.

Sacramento Public Library System: Internet Use and Access Policy

The Library's workstations are in public areas. Since others may be involuntarily exposed to what is viewed, the Library asks that each user exercise good judgment and consideration of others. Please bear in mind that some materials, such as sexually graphic materials, may well be more appropriate for viewing the privacy of your home, rather than in a Public Library setting. If Library staff become aware of subject matter that would interfere with the maintenance of a safe, welcoming, and comfortable environment for the public, the Internet user will be asked to end a search or change a screen. . . . The Sacramento Public Library offers filtered access to the Internet by default. Unfiltered access is available on a per session basis. Juvenile customers under 17 years of age are required to obtain parental consent for unfiltered access on a per session [sic].

San Diego Public Library System: Internet Access Services

On all public terminals, a commercially produced filter is installed to block access to adult-sexually oriented material available through the Internet that might be deemed objectionable. . . . Adults age 17 or older may request staff to disable the Internet filter on any public workstation in the adult Internet area except Express Internet workstations. Internet workstations in children's areas may not have filters disabled. All library policies and guidelines remain in effect and staff will end Internet sessions if inappropriate sites are accessed.

Santa Cruz Public Library System: Internet Access

While protected by the First Amendment to the U.S. Constitution, sexually graphic Internet sites are best suited for private viewing. The Library is a public space. Therefore, viewing sexually graphic Internet sites in the Library is inappropriate. Library users who do so will be asked to stop immediately.

Fresno County Public Library System: Internet Policy

Consistent with Board of Supervisors Policy, federal and state law, all workstations in all branches offer only filtered access to all Library customers of all ages. The Children's Internet Protection Act requires libraries such as the Fresno County Public Library and the other members of the San Joaquin Valley Library System which receive discounts on Internet connections and service to block or filter for all users visual depictions that are obscene or child pornography, and to filter, for minors, depictions which are harmful to minors.

Internet filters are imperfect. They may block some constitutionally protected material, and they may fail to block some unlawful materials. A 2003 U.S. Supreme Court decision authorizes

disabling of the filter for lawful use by adults. Adults 18 years and older may request Library staff to disable the filter for lawful purposes at a specific workstation for a specific session of use. However, no access will be granted to sites rated by the filter as spyware, malware, adware, or the like, because they have the potential to harm the Library's network and/or individual workstations and disrupt the Library's ability to provide service to its users. Phishing sites are blocked because of their deceptive collection of personal information. Please tell Library staff if you believe a site has been rated incorrectly.

Further, if the nature of the content being viewed on the Library workstation disturbs other Library users, the viewer will be asked to cease, to use a privacy screen, or be moved to another workstation.

Shasta County Public Library System: Internet and Computer Use Policy

Through the use of computer software, the Library will filter access by all users to material that meets State and Federal tests for being harmful to a minor. . . . Any person 18 years or over, may, upon request, have the Internet filter disabled to provide access at a terminal of the staff's choosing for bona fide research or other lawful purposes. Viewing of visual depictions of any sexually oriented material for the purpose of appealing to the prurient interests is strictly prohibited.

Attachment D

SUPREME COURT OF THE UNITED STATES
**UNITED STATES et al. v. AMERICAN LIBRARY
ASSOCIATION, INC., et al.**

**APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE EASTERN
DISTRICT OF PENNSYLVANIA**

No. 02—361. Argued March 5, 2003—Decided June 23, 2003

Two forms of federal assistance help public libraries provide patrons with Internet access: discounted rates under the E-rate program and grants under the Library Services and Technology Act (LSTA). Upon discovering that library patrons, including minors, regularly search the Internet for pornography and expose others to pornographic images by leaving them displayed on Internet terminals or printed at library printers, Congress enacted the Children’s Internet Protection Act (CIPA), which forbids public libraries to receive federal assistance for Internet access unless they install software to block obscene or pornographic images and to prevent minors from accessing material harmful to them. Appellees, a group of libraries, patrons, Web site publishers, and related parties, sued the Government, challenging the constitutionality of CIPA’s filtering provisions. Ruling that CIPA is facially unconstitutional and enjoining the Government from withholding federal assistance for failure to comply with CIPA, the District Court held, *inter alia*, that Congress had exceeded its authority under the Spending Clause because any public library that complies with CIPA’s conditions will necessarily violate the First Amendment; that the CIPA filtering software constitutes a content-based restriction on access to a public forum that is subject to strict scrutiny; and that, although the Government has a compelling interest in preventing the dissemination of obscenity, child pornography, or material harmful to minors, the use of software filters is not narrowly tailored to further that interest.

Held: The judgment is reversed.

201 F. Supp. 2d 401, reversed.

Chief Justice Rehnquist, joined by Justice O’Connor, Justice Scalia, and Justice Thomas, concluded:

1. Because public libraries’ use of Internet filtering software does not violate their patrons’ First Amendment rights, CIPA does not induce libraries to violate the Constitution, and is a valid exercise of Congress’ spending power. Congress has wide latitude to attach conditions to the receipt of federal assistance to further its policy objectives, *South Dakota v. Dole*, 483 U.S. 203, 206, but may not “induce” the recipient “to engage in activities that would themselves be unconstitutional,” *id.*, at 210. To determine whether libraries would violate the First Amendment by employing the CIPA filtering software, the Court first examines their societal role. To fulfill their traditional missions of facilitating learning and cultural enrichment, public libraries must have broad discretion to decide what material to provide to their patrons. This

Court has held in two analogous contexts that the Government has broad discretion to make content-based judgments in deciding what private speech to make available to the public. *Arkansas Ed. Television Comm'n v. Forbes*, 523 U.S. 666, 672—674; *National Endowment for Arts v. Finley*, 524 U.S. 569, 585—586. Just as forum analysis and heightened judicial scrutiny were incompatible with the role of public television stations in the former case and the role of the National Endowment for the Arts in the latter, so are they incompatible with the broad discretion that public libraries must have to consider content in making collection decisions. Thus, the public forum principles on which the District Court relied are out of place in the context of this case. Internet access in public libraries is neither a “traditional” nor a “designated” public forum. See, e.g., *Cornelius v. NAACP Legal Defense & Ed. Fund, Inc.*, 473 U.S. 788, 802—803. Unlike the “Student Activity Fund” at issue in *Rosenberger v. Rector and Visitors of Univ. of Va.*, 515 U.S. 819, 834, Internet terminals are not acquired by a library in order to create a public forum for Web publishers to express themselves. Rather, a library provides such access for the same reasons it offers other library resources: to facilitate research, learning, and recreational pursuits by furnishing materials of requisite and appropriate quality. The fact that a library reviews and affirmatively chooses to acquire every book in its collection, but does not review every Web site that it makes available, is not a constitutionally relevant distinction. The decisions by most libraries to exclude pornography from their print collections are not subjected to heightened scrutiny; it would make little sense to treat libraries’ judgments to block online pornography any differently. Moreover, because of the vast quantity of material on the Internet and the rapid pace at which it changes, libraries cannot possibly segregate, item by item, all the Internet material that is appropriate for inclusion from all that is not. While a library could limit its Internet collection to just those sites it found worthwhile, it could do so only at the cost of excluding an enormous amount of valuable information that it lacks the capacity to review. Given that tradeoff, it is entirely reasonable for public libraries to reject that approach and instead exclude certain categories of content, without making individualized judgments that everything made available has requisite and appropriate quality. Concerns over filtering software’s tendency to erroneously “overblock” access to constitutionally protected speech that falls outside the categories software users intend to block are dispelled by the ease with which patrons may have the filtering software disabled. Pp. 6—13.

2. CIPA does not impose an unconstitutional condition on libraries that receive E-rate and LSTA subsidies by requiring them, as a condition on that receipt, to surrender their First Amendment right to provide the public with access to constitutionally protected speech. Assuming that appellees may assert an “unconstitutional conditions” claim, that claim would fail on the merits. When the Government appropriates public funds to establish a program, it is entitled to broadly define that program’s limits. *Rust v. Sullivan*, 500 U.S. 173, 194. As in *Rust*, the Government here is not denying a benefit to anyone, but is instead simply insisting that public funds be spent for the purpose for which they are authorized: helping public libraries fulfill their traditional role of obtaining material of requisite and appropriate quality for educational and informational purposes. Especially because public libraries have traditionally excluded pornographic material from their other collections, Congress could reasonably impose a parallel limitation on its Internet assistance programs. As the use of filtering software helps to carry out these programs, it is a permissible condition under *Rust*. Appellees mistakenly contend, in reliance on *Legal Services Corporation v. Velazquez*, 531 U.S. 533, 542—543, that CIPA’s filtering conditions distort the usual functioning of public libraries. In contrast to the lawyers who furnished legal aid to the indigent under the program at issue in *Velazquez*, public

libraries have no role that pits them against the Government, and there is no assumption, as there was in that case, that they must be free of any conditions that their benefactors might attach to the use of donated funds. Pp. 13—17.

Justice Kennedy concluded that if, as the Government represents, a librarian will unblock filtered material or disable the Internet software filter without significant delay on an adult user's request, there is little to this case. There are substantial Government interests at stake here: The interest in protecting young library users from material inappropriate for minors is legitimate, and even compelling, as all Members of the Court appear to agree. Given this interest, and the failure to show that adult library users' access to the material is burdened in any significant degree, the statute is not unconstitutional on its face. If some libraries do not have the capacity to unblock specific Web sites or to disable the filter or if it is shown that an adult user's election to view constitutionally protected Internet material is burdened in some other substantial way, that would be the subject for an as-applied challenge, not this facial challenge. Pp. 1—2.

Justice Breyer agreed that the "public forum" doctrine is inapplicable here and that the statute's filtering software provisions do not violate the First Amendment, but would reach that ultimate conclusion through a different approach. Because the statute raises special First Amendment concerns, he would not require only a "rational basis" for the statute's restrictions. At the same time, "strict scrutiny" is not warranted, for such a limiting and rigid test would unreasonably interfere with the discretion inherent in the "selection" of a library's collection. Rather, he would examine the constitutionality of the statute's restrictions as the Court has examined speech-related restrictions in other contexts where circumstances call for heightened, but not "strict," scrutiny—where, for example, complex, competing constitutional interests are potentially at issue or speech-related harm is potentially justified by unusually strong governmental interests. The key question in such instances is one of proper fit. The Court has asked whether the harm to speech-related interests is disproportionate in light of both the justifications and the potential alternatives. It has considered the legitimacy of the statute's objective, the extent to which the statute will tend to achieve that objective, whether there are other, less restrictive ways of achieving that objective, and ultimately whether the statute works speech-related harm that is out of proportion to that objective. The statute's restrictions satisfy these constitutional demands. Its objectives—of restricting access to obscenity, child pornography, and material that is comparably harmful to minors—are "legitimate," and indeed often "compelling." No clearly superior or better fitting alternative to Internet software filters has been presented. Moreover, the statute contains an important exception that limits the speech-related harm: It allows libraries to permit any adult patron access to an "overblocked" Web site or to disable the software filter entirely upon request. Given the comparatively small burden imposed upon library patrons seeking legitimate Internet materials, it cannot be said that any speech-related harm that the statute may cause is disproportionate when considered in relation to the statute's legitimate objectives. Pp. 1—6.

Rehnquist, C. J., announced the judgment of the Court and delivered an opinion, in which O'Connor, Scalia, and Thomas, JJ., joined. Kennedy, J., and Breyer, J., filed opinions concurring in the judgment. Stevens, J., filed a dissenting opinion. Souter, J., filed a dissenting opinion, in which Ginsburg, J., joined.

Attachment E

November 29, 2006 Report

http://abclocal.go.com/kgo/story?section=i_team&id=4808374

Porn, Sex Crimes At Libraries **I-Team Investigation**



By Dan Noyes

Nov. 29 - KGO - You expect a public library to be a safe, clean place for everyone -- children included. But that's not what the I-Team caught on tape during a survey of libraries around the Bay Area.

Over the course of three weeks, we took our cameras to the Bay Area's main libraries. If you haven't been to a public library in a while, you might be surprised by what we found.

One word of caution -- some of what the I-Team captured on tape is graphic.

It's opening time at the San Francisco main library. The crowd swarms in. Some unpack their bags and settle in for a long day. They aren't there for the books or computers. The library gives them a chance to get off the streets.

The I-Team found people tucked away in corners and asleep out in the open. One man stripped to his underwear and changed clothes, in full view, between the stacks of books.

Luis Herrera, San Francisco librarian: "It's not acceptable in the library."

City librarian Luis Herrera says all this activity is against the rules.

Luis Herrera, San Francisco librarian: "What should have happened here is our staff, anybody that notices that, should immediately bring it to our attention, so we can call security and it's irresponsible not to respond to a situation like this."

During our surveillance, we saw no guards patrolling the floors. They remained at the front entrance.

After we filed a public records request for the library's incident reports, Herrera brought in a sergeant from the S.F.P.D. to reorganize his security force.

It's a frustrating situation for the staff.

According to a library survey completed in September, among the most common responses:

"Unpleasant behaviors drive away well behaved patrons."

"I feel my safety and health are at risk on a daily basis."

It's not just the staff who feel threatened.

Mother: "We don't go to that library anymore."

This woman's 11-year-old daughter got punched at the library in January by a mentally-disturbed woman. She's not showing her face or using her name to protect her daughter. They live and work in the neighborhood.

Mother: "You don't take your children to the library to get punched, you know? The library's not a safe place. It's more like a hangout place. People drop their kids off because parents are working and there's nobody to look out."

A review of the past year's police logs shows assaults, lewd acts, and drug use. These are problems we also found in San José. And the Martin Luther King Library has a problem with pornography. They have no rule against viewing photographs or full-screen sex videos from Internet sites, even with children nearby.

Chief librarian Jane Light says it's a matter of free speech.

Jane Light, San José librarian: "If anyone objects, doesn't like that because they're seeing something they don't want to see, they just let us know and the customer will be required to place a screen on their screen that means people can't see it from the side."

But take a look at the privacy screens. They block the view if you're sitting next to the computer, but if you move back just a bit and the picture's clear again.

Doug Smith, Oakland librarian: "It really only offers partial privacy."

ABC7's Dan Noyes: "I've seen the screens and I see how they work and the stuff is visible from behind. You can see everything."

Jane Light, San José librarian: "So you can avert your eyes. It's really & we have a great children's room. I don't know if you've seen our children's room."

Yes, the library does have a room set aside for kids, but they aren't required to go there. They can wander to any floor, even where we spotted a man viewing child porn on a library computer right out in the open.

San José's police blotter over the past year lists several arrests for child porn at the library, at least ten cases of child molestation or other sex crimes involving kids and several cases of men viewing porn and performing a lewd act, right at the terminal.

Guards caught this man on surveillance camera.

Sgt. John Laws, San José library police: "It showed him sitting at the computer terminal and from our vantage point it appeared to show movement that was consistent with him masturbating."

He was convicted by a jury in September of a lewd act in public and sentenced to 30 days in the county jail.

Records show the same thing happens in San Francisco quite often. In fact, we stumbled upon a man committing a lewd act on the floor. And we found another man in the library's teen section cruising porn sites while two boys played computer games just across the same table. No one said anything and we watched him for more than an hour. He continued on the sex sites even after spotting our camera.

We taped another man at a crowded table watching graphic, full-screen sex videos. The librarians were just across the aisle.

ABC7's Dan Noyes: "Porn is available on there. Kids can see this as they walk by. Is this a safe place for kids?"

Luis Herrera, San Francisco librarian: "I can't guarantee safety, but I would venture to say that it is a safe place for kids."

Marcia Stacke, Child Quest International: "It stuns me that that is going on in our public libraries today."

Marcia Stacke runs Child Quest International out of this San José office. They sponsor child protection programs, help find missing kids and campaign for Internet safety. Stacke says something has to be done.

Marcia Stacke, Child Quest International: "You know, sometimes I wonder if we're just too afraid to be, I don't know, sued in this country. We've got to step out and protect our kids. Enough is enough."

Stacke believes that more libraries should filter out pornographic sites on their computers. Forty percent of the libraries across the country use some level of filters on their computers but not San Francisco, San José or Oakland.

This California state librarian tells us filtering is not a fast and easy answer.

Susan Hildreth, CA state librarian: "Internet filtering is not 100 percent effective at all. They're not able to deal with all the wild and crazy sites that are put up at every minute of the day."

We found a good solution in Oakland -- an attentive staff. This main library fared the best out of the three we surveyed. We spotted fewer cases of inappropriate behavior during our surveillance, and in a search of police records.

Doug Smith, Oakland librarian: "We will approach people and intervene when necessary. We really try and establish an atmosphere of safety here."

If you're concerned about these issues, the experts say you should stick to the smaller branch libraries, where the staff can keep a better handle on what's happening in their building.

And don't leave your kids alone at the library if they aren't old enough to handle a difficult situation.

Attachment F

December 1, 2006 Report

http://abclocal.go.com/kgo/story?section=i_team&id=4815686

Fallout Follows I-Team Library Investigation **S.J. Mayor-Elect To Take Action**



By Dan Noyes

Dec. 1 - KGO - The library community is buzzing about an I-Team investigation that exposed sex crimes and pornography in the Bay Area's main libraries. San José's mayor-elect is pledging to take action after seeing the report.

The report has touched a nerve. In the past two days, we've been getting e-mail from outraged parents and library staff who are glad we finally told the story. This has been one of those secrets that no one wanted to talk about.

Chuck Reed, San José Mayor-elect: "It may not be a crime, but it's not something we have to tolerate."

We played our investigation on our video player on abc7news.com for San José Mayor-elect Chuck Reed.

We found problems at the Martin Luther King main library, especially pornography. They have no rule against viewing photographs or full-screen sex videos from Internet sites, even with children nearby.

Police records and surveillance tapes show several men have been arrested in the past year for viewing porn out in the open and performing lewd acts.

Now Reed says one of his first tasks when he takes over as mayor will be to launch his own investigation into the issue, and consider moving the library's computers.

Chuck Reed, San José Mayor-elect: "That would be important to try to have a setup that makes it more difficult for bad things to happen and makes it easier for our librarians to correct them when they do."

Since the I-Team story aired Wednesday, we've received several e-mails from staff at the library who say they don't like being exposed to porn, especially the child porn we spotted, on a daily basis and that it's a hostile work environment.

Erik Larsen, S.J. City Employees Union President: "It is uncomfortable for employees to be in that position."

The city employees union president says it's especially disturbing because so many jobs have been cut since the dot-com bust. The library is counting on 15 and 16-year-old pages to do a lot of the work, and they're having to deal with the porn.

Erik Larsen, S.J. City Employees Union President: "You can't have young folks under the age of 18 monitoring children or adults when it comes to this type of issue with pornography."

In our investigation Wednesday, chief librarian Jane Light defended access to Internet porn as a matter of free speech.

Jane Light, San José librarian: "If anyone objects, doesn't like that because they're seeing something they don't want to see, they just let us know and the customer will be required to place a screen on their screen. That means people can't see it from the side."

But take a look at the privacy screens. They block the view if you're sitting next to the computer. But if you move back just a bit, the picture's clear again.

Mayor-elect Reed sees porn and the right to free speech differently than the chief librarian.

Chuck Reed, San José Mayor-elect: "There are limits on free speech. There's no constitutional right that's absolute and free speech is not an absolute right. No one has a right to expose other people to pornography."

Forty percent of the public libraries in this country use some sort of filters on their computers to limit access to pornography -- but not San José. The American Civil Liberties Union has fought filters in libraries.

Nicole Ozer, ACLU Technology Policy Director: "Just like we don't censor the types of books that we have in the library, we don't censor the type of information that's available on the Internet sites in the library."

The ACLU's technology policy director says the key is an attentive staff and attentive parents.

Nicole Ozer, ACLU Technology Policy Director: "Just like you wouldn't want your child to necessarily be able to look at any book that's on the stack, you might want to accompany them and be sure that they're looking at the right kind of books in the library, that they're in the right place in the library."

And the right kind of websites. Our investigation also showed there have been at least 10 cases of child molestation or other sex crimes involving kids over the past year at the San José main library.

The I-Team tried to reach San Francisco Mayor Gavin Newsom today about the problems we found at his city's main library. His staff did not return our phone calls or e-mail requesting an interview.

Attachment G

PROPOSED CITY INTERNET ACCESS POLICY

The purpose of the Dr. Martin Luther King Jr. Library and the San José Public Library system is to facilitate educational and informational pursuits by furnishing materials of requisite and appropriate quality. The Library provides public access to the Internet to further this purpose. The Internet offers links to a vast array of valuable local, national, and international sources of information that may not otherwise be found in the system's collection. However, because the Internet is a vast and unregulated medium, the Library has limited control over the information available through the Internet and is not responsible for the accuracy, authenticity, or timeliness of its content.

Responsibilities of Users

All users of San José Public Library computers or networks are expected to use the Internet in a manner consistent with the purpose for which it is provided and according to the guidelines established by the Library. Use of Library computers for unlawful purposes will result in an immediate revocation of computer privileges.

All Library computers terminals shall display the following warning:

Library users may not use San José Public Library computers for unlawful purposes or to view illegal content. Users who view or receive illegal content on library computers may be subject to federal criminal prosecution.

The Library uses technology protection measures to filter Internet content in accordance with federal law. However, the San José Public Library system cannot guarantee that the filter will block all materials deemed objectionable. Users who encounter objectionable material may submit a request to the Library for those sites to be filtered. Parents and legal guardians must assume responsibility for guiding their children's Internet usage. For more information on children and the Internet, parents and legal guardians are encouraged to visit [My Rules for Internet Safety](#).

Additionally, all users must abide by the following rules:

1. Due to the limited resources available for provision of public access to the Internet, the Library reserves the right to limit the amount of time an individual user may have access to library equipment.
2. Rules for use of the Library's Internet workstations are posted near or on terminals, and include reservation information, time limits on usage of machines, and limits on printing.
3. Library staff members will assist customers, as time permits, with basic Internet navigation and with basic computer and printer functions.
4. Users may not attempt to reconfigure systems or software, or in any way interfere with or disrupt the current system or network set-up and services.

5. Users may not damage, alter, or degrade computer equipment, peripherals, or configurations.
6. Some workstations have a dedicated purpose, such as searching for periodical citations and articles, and are to be used only for that dedicated purpose. Some workstations are reserved for use by children or for use by people with disabilities.
7. Users may not view, print, distribute, display, send, or receive obscene material or material that constitutes child pornography. Users also may not disseminate, exhibit, or display to minors materials that are harmful to minors.
8. Privacy screens are available in all branches and units of the Library, and may be requested by customers for use in the library. In addition, a staff member may require a customer to use a privacy screen when a staff member deems it necessary.
9. Users may not invade the privacy of others. Each customer has the right to a quiet and organized work space. No more than two people may use a work station at the same time.
10. If any user abuses or engages in unauthorized use of computers, his or her computer privileges will be denied. If a customer refuses a staff request to end problem behavior, the customer will be asked to leave the library. Staff may call upon the assistance of other and/or supervisory staff, and if the situation escalates, Public Safety staff or police may be called.
11. Computers will be shut down no later than 5 minutes before the library closes.

Internet Filtering

The Library uses filtering technology on all computers with Internet access. Patrons 17 years of age or older are given a choice of an Internet session with a basic filter or one that has additional filtering. The intent of the basic filter is to block websites that contain child pornography or material that is obscene.

The intent of the additional filtering is to block websites that contain material that is harmful for minors. If a patron 17 years of age or older wishes to access a blocked site for bona fide research or other lawful purpose, he or she may request that the site be unblocked either temporarily or permanently. All Library Policies shall remain in effect. For a temporary unblock request, the patron should make the request to a library employee, who will refer it to the IT specialist on duty. If the IT specialist determines that the site is appropriate for viewing (i.e. falls outside the appropriate filtering categories) the site will be unblocked for 24 hours.

If a patron wishes to permanently unblock a site, he or she may submit a written request to the library. The library will forward the request to the software provider. If the provider believes that the site should remain blocked according to the criteria discussed in the previous two paragraphs, the patron may seek review by a team of three library employees. The library employees may review the site and recommend to the provider that the site be unblocked. Upon review, if the software provider decides that the site should remain blocked, it will submit its decision to the library team in writing with reasons for its decision. The provider's decision is final.

Patrons 16 years of age or younger must use the additional filtering, and are required to obtain consent from a parent or legal guardian before requesting a site to be unblocked. Library staff may request proof of age.

Given the nature of how information and sites become accessible through the Internet, the San José Public Library system cannot guarantee that the filtering technology will block all material deemed objectionable. Users who encounter objectionable material may submit a request to the Library for those sites to be filtered.

Supervising Children's Internet Use

Parents and legal guardians must assume responsibility for overseeing their child's exposure to and use of the Internet. While the Library has installed filtering software in accordance with federal law, filters will not necessarily prevent children from accessing all Internet materials that a parent might find objectionable. The filtering software is not a substitute for individual judgment and parental involvement.

The Library has created Web pages for children ([KidsPlace](#)) and young adults ([TeenWeb](#)) which provide content and links to other Web sites that parents and legal guardians may find appropriate for their children. For more information on children and the Internet, parents and legal guardians are encouraged to visit [My Rules for Internet Safety](#).

If a library cardholder is under the age of 18, the parent or legal guardian who signed for the child's card may be given specific information regarding that child's record. If the parent or guardian is in possession of the child's card, they may be given any information in the child's record, including Internet usage. If the child's card is not in the parent's or guardian's possession, the information provided will be limited to (1) materials that are overdue, lost, or damaged, and (2) fines owed.